## WHAT IS CLAIMED IS:

1. A method for updating a program in a data processing system comprising the steps of:

requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program;

the TPM performing the signature verification of the update to the program;

if the signature verification of the update to the program is successful, unlocking a memory unit storing the program; and

modifying the program with the update to the program in response to the unlocking of the memory unit storing the program.

2. The method as recited in claim 1, further comprising the step of:

locking the memory unit after the modifying step.

3. The method as recited in claim 2, wherein the locking step is performed by the TPM.

4. A computer program product adaptable for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

a BIOS update application program receiving an updated BIOS image;

the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image;

a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image; and

the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application.

5. The computer program product as recited in claim 4, further comprising:

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory; and

the BIOS update application modifies the BIOS with the updated BIOS image.

6. The computer program product as recited in claim 5, further comprising:

programming for locking the flash memory after the BIOS update application modifies the BIOS with the updated BIOS image.

7. The computer program product as recited in claim 6, further comprising:

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output.

8. A data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising:

input circuitry for receiving an updated BIOS image;

circuitry for requesting a TPM to perform a signature verification of the updated BIOS image;

the TPM performing the signature verification of the updated BIOS image;

the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic; and

circuitry for modifying the BIOS with the updated BIOS image.

9. The system as recited in claim 8, further comprising:

circuitry for locking the flash memory after the BIOS is modified with the updated BIOS image.

10. The system as recited in claim 8, further comprising:

circuitry for outputting an error if the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic.